Duality Preserving Gray Maps for Codes over Rings

Steve Szabo *
Department of Mathematics and Statistics
Eastern Kentucky University
Richmond, KY 40475

Felix Ulmer†
IRMAR, CNRS, UMR 6625
Université de Rennes 1
Université européenne de Bretagne
Campus de Beaulieu, F-35042 Rennes

Abstract

Given a finite ring A which is a free left module over a subring R of A, two types of R-bases, pseudo-self-dual bases (similar to trace orthogonal bases) and symmetric bases, are defined which in turn are used to define duality preserving maps from codes over A to codes over R. Both types of bases are generalizations of similar concepts for fields. Many illustrative examples are given to shed light on the advantages to such mappings as well as their abundance.

Keywords: Codes over Rings, Self-Dual Codes, Trace Orthogonal Basis, Symmetric Basis, Codes over Noncommutative Rings. MSC2010: 94B05, 94B60

1 Introduction and Overview

Codes over rings have been a major topic in coding theory ever since the discovery of the connection between linear codes over $\mathbb{Z}_4$ to some good non-linear binary codes in [8]. They showed that there is a Gray map from codes over $\mathbb{Z}_4$ to codes over $\mathbb{F}_2^2$ for which the mentioned good non-linear codes were the images of linear $\mathbb{Z}_4$ codes. Many classical constructions of codes over fields like cyclic codes and geometric codes have been generalized to rings ([4, 12]). The idea of mapping codes from larger rings onto codes over smaller rings has been a growing topic where not only non-linear but also linear mappings are used.

*e-mail: steve.szabo@eku.edu
†e-mail: felix.ulmer@univ-rennes1.fr

Example 1.1. Consider the $\mathbb{F}_2$-algebra $A = \mathbb{F}_2[x]/(x^2)$ (see [9]). Using the ordered $\mathbb{F}_2$ basis $\mathcal{B} = (1, x)$ of A, any n-length code over A can be mapped to a $2n$-length code over $\mathbb{F}_2$ via the bijective Gray map

$$\Phi_{\mathcal{B}} : A^n \to (\mathbb{F}_2)^{2n};\ (a_1, a_2, \ldots, a_n) \to (\alpha_{1,1}, \alpha_{1,2}, \alpha_{2,1}, \alpha_{2,2}, \ldots, \alpha_{n,1}, \alpha_{n,2})$$

where $a_i = \alpha_{i,1} + \alpha_{i,2}x$ is the representation of a_i in the basis $(1, x)$. The image $\Phi_{\mathcal{B}}(C)$ of a linear code C over A is a code over $\mathbb{F}_2$. Specifically, consider $g = X^2 + xX + 1 \in A[X]$. This polynomial is a divisor of $X^4 - 1 \in A[X]$ and generates a cyclic code $C = (g)/(X^4 - 1) \subset A[X]/(X^4 - 1)$ of length 4 over A. In the standard correspondence of $(g)/(X^4 - 1)$ with A^4, g corresponds to the code word $w_g = (1, x, 1, 0)$ which is mapped to $\Phi_{\mathcal{B}}(w_g) = (1, 0, 0, 1, 1, 0, 0, 0)$. Also, the code word $x \cdot (X^2 + xX + 1)$ is mapped to $(0, 1, 0, 0, 0, 1, 0, 0)$. Applying this argument to the code word $X \cdot g$ we see that

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

is a generator matrix of the binary image $\Phi_{\mathcal{B}}(C)$ of C.

Self-dual codes have become a central topic in coding theory due to their connections to other fields of mathematics such as block designs [6]. In many instances, self-dual codes have been found by first finding a code over a ring and then mapping this code onto a code over a subring through a map that preserves duality. Often, these maps have been found through ad hoc methods. For instance, in [14], the local Frobenius non-chain rings of order 16 were found and a map that preserves duality was presented for each ring. In the literature, the mappings typically map to codes over $\mathbb{F}_2$, $\mathbb{F}_4$ and $\mathbb{Z}_4$ since codes over these rings have had the most use.

Example 1.2. We consider again the cyclic code $C = (g)/(X^4 - 1) \subset A[X]/(X^4 - 1)$ of length 4 over $A = \mathbb{F}_2[x]/(x^2)$ generated by $g(X) = X^2 + xX + 1 \in A[X]$. Since g equals its reciprocal polynomial $X^2 \cdot g(1/X)$, the code C is self-dual of length 4 over A. However, the binary image $\Phi_{\mathcal{B}}(C)$ of C obtained in previous example using the basis $\mathcal{B} = (1, x)$ is not a self-dual binary code. If we use the $\mathbb{F}_2$-basis $\mathcal{B}' = (1, x + 1)$ to map to $\mathbb{F}_2^8$, then the image $\Phi_{\mathcal{B}'}(C)$ of C is the type II binary code $[8, 4, 4]_2$ generated by

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Note that the code word $(1, x, 1, 0)$ corresponding to $g \in A[X]/(X^4 - 1)$ can be written $(1 \cdot 1 + 0 \cdot (x + 1), 1 \cdot 1 + 1 \cdot (x + 1), 1 \cdot 1 + 0 \cdot (x + 1), 0 \cdot 1 + 0 \cdot (x + 1))$ and maps to the first row $(1, 0, 1, 1, 1, 0, 0, 0)$, while the second row is the image

of $(1+x)\cdot g$. It is well known ([9]) that in the $\mathbb{F}_2$-basis $\mathcal{B}' = (1, x+1)$ of A, the image of a self-dual code over A under $\Phi_{\mathcal{B}'}$ is always a self-dual code over $\mathbb{F}_2$. Therefore, the mapping corresponding to the basis $\mathcal{B}' = (1, x+1)$ preserves duality.

A duality preserving Gray map does not always exist (see [15]). We aim to give criteria for bases which guarantee that the corresponding Gray map Φ preserves duality. Our setting is as described above: A is a finite ring that is a free left module over a subring R of A. We present two types of bases that have this duality preserving property. The first, *pseudo-self-dual bases*, are a generalization of trace orthogonal bases which have been defined for algebras over finite fields in [17] and [5]. The second, *symmetric bases*, are a generalization of the same for finite fields defined in [16]. In the case of symmetric bases, it is required that A, not only be a left R-module, but a left R-algebra which in turn then requires that $R \subset Z(A)$.

Other than in [2], where a criterion is given to find a basis for $\mathbb{F}_q[x]/(x^t)$ that maps self-dual codes over $\mathbb{F}_q[x]/(x^t)$ to self-dual codes over $\mathbb{F}_q$, the authors are unaware of general methods for finding duality preserving maps. The methods herein are much more general than that in [2]. It is shown here that the criteria for an $\mathbb{F}_q$-basis for $\mathbb{F}_q[x]/(x^t)$ to preserve duality given in [2] is equivalent to the basis being symmetric (see Proposition 3.20).

The paper is organized as follows: Section 2 contains preliminaries and definitions needed throughout the rest of the paper. Section 3 lays out the two methods for finding duality preserving bases. In section 4 we study the behavior of self-dual cyclic codes under duality preserving Gray maps and show that some Gray maps are better than others in terms of hamming distance for this family of codes.

2 Preliminaries

For a ring A, $Aut(A)$ is the **automorphism group** of A, a subset C of A^n is an n **length code over** A and if C is a left A-submodule of A^n then C is an A**-linear code** over the alphabet A. For a finite ring A and a subgroup H of $Aut(A)$, the **fixed subring** of H is $A^H = \{a \in A | h(a) = a \text{ for all } h \in H\}$ and the **trace function with respect to** H is

$$Tr_H : A \to A;\ a \mapsto \sum_{h \in H} h(a).$$

Lemma 2.1. *Let A be a ring and H be a subgroup of $Aut(A)$. The trace function with respect to H is both a left and right A^H-linear map and for $a \in A$, $Tr_H(a) \in A^H$.*

Proof. Let $a \in A$, $b \in A^H$ and $g \in H$. Then

$$Tr_H(ba) = \sum_{h \in H} h(ba) = \sum_{h \in H} h(b)h(a) = \sum_{h \in H} bh(a) = b\left(\sum_{h \in H} h(a)\right).$$

So, Tr_H is left A^H-linear. Similarly, Tr_H is right A^H-linear. Also,

$$g(Tr(a)) = g\left(\sum_{h\in H} h(a)\right) = \sum_{h\in H} g(h(a)) = \sum_{h\in H} h(a) = Tr(a)$$

showing $Tr_H(a) \in A^H$. □

For a ring A, an anti-automorphism σ on A and a left A-module M, a **σ-sesquilinear form** on M is a map $\langle\cdot,\cdot\rangle : M \times M \to A$ such that if $x, y, z \in M$ and $a \in A$ then $\langle x+z, y\rangle = \langle x, y\rangle + \langle z, y\rangle$, $\langle x, y+z\rangle = \langle x, y\rangle + \langle x, z\rangle$, $\langle ax, y\rangle = a\langle x, y\rangle$ and $\langle x, ay\rangle = \langle x, y\rangle\sigma(a)$. In addition, if $\sigma(\langle x, y\rangle) = \langle y, x\rangle$ then the form is called a **σ-hermitian form**. A σ-sesquilinear form with the property that $\langle x, y\rangle = 0 \iff \langle y, x\rangle = 0$ is called **reflexive**. Clearly a σ-hermitian form is reflexive.

Proposition 2.2. *Let A be a ring and σ be an anti-automorphism on A. Define the map*

$$\langle\cdot,\cdot\rangle : A^k \times A^k \to A; \quad \langle x, y\rangle = \sum_{i=1}^{k} x_i\sigma(y_i).$$

Then $\langle\cdot,\cdot\rangle$ is a σ-sesquilinear form. Furthermore, $\langle\cdot,\cdot\rangle$ is a σ-hermitian form if and only if σ is involutory, i.e. $\sigma^2 = id$.

Proof. Clearly, $\langle\cdot,\cdot\rangle$ is a σ-sesquilinear form. Assume $\langle\cdot,\cdot\rangle$ is hermitian. For $a \in A$, $a = a\langle(1, 0, \ldots, 0), (1, 0, \ldots, 0)\rangle = \langle(a, 0, \ldots, 0), (1, 0, \ldots, 0)\rangle$. Since σ is hermitian, $\sigma^2(a) = \sigma^2(\langle(a, 0, \ldots, 0), (1, 0, \ldots, 0)\rangle) = a$ showing σ is involutory.

Now, assume σ is involutory. For $x, y \in A^k$, $\sigma(\langle x, y\rangle) = \sigma(\sum_{i=1}^k x_i\sigma(y_i)) = \sum_{i=1}^k \sigma(x_i\sigma(y_i)) = \sum_{i=1}^k y_i\sigma(x_i) = \langle y, x\rangle$ showing $\langle\cdot,\cdot\rangle$ is σ-hermitian. □

When the form in Proposition 2.2 is hermitian, it is known as the **standard σ-hermitian form** on A^k which we denote as $\langle x, y\rangle_{A^k}$. If σ is the identity map, $\langle x, y\rangle_{A^k}$ is known as the **standard bilinear form** on A^k. In the following an involution denotes an anti-automorphism of order 1 or 2. Since the identity map is an involution if and only if A is commutative, we may only consider the standard bilinear form on A^k when A is commutative. If R is a subring of A such that $\sigma(R) = R$ then $\sigma|_R$ is an involution on R. Then, if entries in A^k are restricted to R^k, the standard σ-hermitian form on A^k is the standard $\sigma|_R$-hermitian form on R^k.

We will specialize to the standard σ-hermitian form on A^k for which we define the orthogonal of a code. From Proposition 2.2, we know then that σ is an involution. For a finite ring A, the standard σ-hermitian form on A^k and an A-linear code $C \subset A^k$, the **dual code** of C, denoted by $C^\perp$, is $C^\perp = \{v \mid \langle v, c\rangle_{A^k} = 0, \forall c \in C\}$. It is immediate that $C^\perp$ is a left A-module, therefore also an A-linear code. A code is **self orthogonal** if $C \subset C^\perp$ and **self dual** if $C = C^\perp$.

The dual we have defined is typically referred to as the left dual. There is an analog notion of a right dual. These of course when working over a commutative

ring are identical. Furthermore, since we have defined the dual based on a hermitian form and a hermitian form is reflexive (see definition above), the left and right duals coincide over non-commutative rings as well, that is

$$\{v \mid \langle v, c\rangle_{A^k} = 0, \forall c \in C\} = \{v \mid \langle c, v\rangle_{A^k} = 0, \forall c \in C\}.$$

In [19], Wood showed, amongst other fundamental results on codes over Frobenius rings, that using the standard bilinear form to define the dual $C^\perp$ of an n-length linear code C over a Frobenius ring A, $|C||C^\perp| = |A|^n$. This result was extended in [18] to bilinear forms and sesquilinear forms in general. The following is a specialization of that result to our setting.

Lemma 2.3. *Let A be a finite Frobenius ring and C be a linear code over A. Then $|C||C^\perp| = |A|^n$.*

For this and other reasons presented in [19], most coding theorists restrict their study to codes over Frobenius rings. For the definition and details about Frobenius rings see [19]. We will keep things general and not restrict the development of the theory to Frobenius until necessary. To illustrate one of the difficulties of working on codes over non-Frobenius rings we provide the following example.

Example 2.4. Let $A = \mathbb{F}_2[u, v]/(u^2, v^2, uv)$ which is of order 8. The Jacobson radical of A is $J(A) = (u, v)$ and the socle of A is $S(A) = (u, v)$. A finite Frobenius ring R can be characterized by having the property that $R/J(R) \cong S(R)$ as left R-modules. We see that as A-modules, $A/J(A) = \{J(A), 1 + J(A)\} \cong \mathbb{F}_2$ but $Soc(R) = (u) + (u + v) + (v) \cong \mathbb{F}_2^3$. So, A is non-Frobenius. Consider the ideal $C = (u, v) \lhd A$ as a 1-length code over A. We see that $C = C^\perp$. So, $|C||C^\perp| = 16 > 8 = |A|$.

3 Duality Preserving Bases

Throughout this section let $n \in \mathbb{N} \setminus \{0\}$, let A be a finite unitary ring which is a free left module over a unitary subring R of A, $\mathcal{B} = (v_1, \ldots, v_r)$ be an ordered left R-basis for A and σ be an involution on A such that $\sigma(R) = R$. Define the maps

$$\rho : A \to R^r; \quad \alpha_1 v_1 + \cdots + \alpha_r v_r \mapsto (\alpha_1, \ldots, \alpha_r)$$

and

$$\Phi : A^n \to R^{rn}; \quad (a_1, \ldots, a_n) \mapsto (\rho(a_1), \ldots, \rho(a_n)).$$

Typically, the map Φ is called a Gray map. With it, we define the **Gray weight on A with respect to $\mathcal{B}$** as follows: For $z \in A^n$, $W_{\mathcal{B}}(z) = w_H(\Phi(z))$ where w_H is the Hamming weight on R^{rn}. Given a code C over A, for every R-basis of A there is an image viewed through this basis and a weight function with respect to this basis for which Φ becomes an isometry. The next example illustrates this.

Example 3.1. Assume $A = \mathbb{F}_2 \times \mathbb{F}_2$. Any two non-zero elements of A form an $\mathbb{F}_2$-basis. Let $\mathcal{C} = \{(1,0),(0,1)\}$, $\mathcal{D} = \{(1,0),(1,1)\}$ and $\mathcal{E} = \{(1,1),(0,1)\}$. Then for the codeword of length 2 over A, $c = ((1,0),(1,0),(0,1))$, $\Phi_{\mathcal{C}}(c) = (1,0,1,0,0,1), \Phi_{\mathcal{D}}(c)) = (1,0,1,0,1,1)$ and $\Phi_{\mathcal{E}}(c)) = (1,1,1,1,1,0)$. So, $W_{\mathcal{C}}(c) = 3$, $W_{\mathcal{D}}(c) = 4$ and $W_{\mathcal{E}}(c) = 5$.

Before moving on, we show the connection between the inner product on A^n and the inner product on R^{rn}. To that end we introduce the following, let

$$M = \mathcal{B}^T \sigma(\mathcal{B}) = \begin{pmatrix} v_1\sigma(v_1) & \dots & v_1\sigma(v_r) \\ \vdots & \vdots & \vdots \\ v_r\sigma(v_1) & \dots & v_r\sigma(v_r) \end{pmatrix},$$

and let $\mathcal{M}$ be the block diagonal $nr \times nr$ matrix with M on the diagonal.

Lemma 3.2. *Let $x, y \in A^n$. Then $\langle x, y \rangle_{A^n} = \Phi(x)\mathcal{M}\sigma(\Phi(y))^T$.*

Proof. Let x_i and y_i be the i-th component of x and y respectively. Note that for $a \in A$, $a = \rho(a)\mathcal{B}^T$. Then

$$\begin{aligned} \langle x, y \rangle_{A^n} &= \sum_{i=1}^{n} x_i\sigma(y_i) = \sum_{i=1}^{n} \rho(x_i)\mathcal{B}^T\sigma(\rho(y_i)\mathcal{B}^T) = \sum_{i=1}^{n} \rho(x_i)\mathcal{B}^T\sigma(\mathcal{B})\sigma(\rho(y_i))^T \\ &= \sum_{i=1}^{n} \rho(x_i)M\sigma(\rho(y_i))^T = \Phi(x)\mathcal{M}\sigma(\Phi(y))^T \end{aligned}$$

□

In this section we investigate the sufficient conditions on $\mathcal{B}$ so that $\langle x, y \rangle_{A^n} = 0$ implies $\langle \Phi(x), \Phi(y) \rangle_{R^{nr}} = 0$ giving a so called duality preserving basis. We will give two separate conditions on $\mathcal{B}$ that guarantee it will preserve duality.

3.1 Pseudo-Self-dual Bases

In this subsection we consider pseudo-self-dual bases and show that such bases preserve duality. In [17], trace orthogonal bases for finite field extensions were defined. We extend this definition to include ring extensions in our setting as we consider the extension $A \supset R$.

Definition 3.3. For a subgroup H of $Aut(A)$ we define the following. $\mathcal{B}$ is a **σ-trace orthogonal basis** with respect to H if for $1 \le i, j \le r$, $Tr_H(v_i\sigma(v_j)) = 0$ if and only if $i \neq j$. In addition, if there exists $\gamma \in A$ that is not a zero divisor, commutes with elements of R and $Tr_H(v_i\sigma(v_i)) = \gamma$ for $1 \le i \le r$ then $\mathcal{B}$ is called a **σ-pseudo-self-dual basis** with respect to H. Furthermore, if $\gamma = 1$, $\mathcal{B}$ is called a **σ-self-dual basis** with respect to H.

Table 1: Number of σ-pseudo-self-dual bases w.r.t. H of $\mathbb{F}_3(\xi)[x]/(x^2+1)$ over R

σ \ H	$\langle\psi\rangle$	$\langle\theta^2\rangle$	$\langle\theta^2\psi\rangle$	$\langle\theta\psi\rangle$	$\langle\theta^3\psi\rangle$	$\langle\theta\rangle$	$\langle\psi,\theta^2\rangle$	$\langle\theta\psi,\theta^2\rangle$	$Aut(A)$
id	64	0	32	0	0	112	112	0	112
ψ	64	16	64	0	0	112	112	16	112
θ^2	96	64	64	0	0	96	96	64	96
$\theta^2\psi$	96	32	0	0	0	96	96	32	96
$\theta\psi$	32	0	32	0	0	352	352	0	352
$\theta^3\psi$	32	0	32	0	0	352	352	0	352

(a) $R = \mathbb{F}_3(\xi)$

σ \ H	$\langle\psi\rangle$	$\langle\theta^2\rangle$	$\langle\theta^2\psi\rangle$	$\langle\theta\psi\rangle$	$\langle\theta^3\psi\rangle$	$\langle\theta\rangle$	$\langle\psi,\theta^2\rangle$	$\langle\theta\psi,\theta^2\rangle$	$Aut(A)$
id	32	0	64	0	0	112	112	0	112
ψ	0	32	96	0	0	96	96	32	96
θ^2	64	64	96	0	0	96	96	64	96
$\theta^2\psi$	64	16	64	0	0	112	112	16	112
$\theta\psi$	32	0	32	0	0	352	352	0	352
$\theta^3\psi$	32	0	32	0	0	352	352	0	352

(b) $R = \mathbb{F}_3(x+1)$

σ \ H	$\langle\psi\rangle$	$\langle\theta^2\rangle$	$\langle\theta^2\psi\rangle$	$\langle\theta\psi\rangle$	$\langle\theta^3\psi\rangle$	$\langle\theta\rangle$	$\langle\psi,\theta^2\rangle$	$\langle\theta\psi,\theta^2\rangle$	$Aut(A)$
id	0	0	0	0	0	96	96	0	96
ψ	0	0	0	0	0	96	96	0	96
θ^2	0	0	0	0	0	96	96	0	96
$\theta^2\psi$	0	0	0	0	0	96	96	0	96
$\theta\psi$	0	0	0	0	0	0	0	0	0
$\theta^3\psi$	0	0	0	0	0	0	0	0	0

(c) $R = \mathbb{F}_3$

A gray highlighted involution σ indicates that $\sigma(R) = R$ and a gray highlighted subgroup H indicates that H fixes R element-wise.

Example 3.4. Assume $A = \mathbb{F}_3(\xi)[x]/(x^2+1)$ where $\xi^2 + 2\xi + 2 = 0$. Note, $\mathbb{F}_3(\xi) \cong \mathbb{F}_9$. Since $x^2 + 1 = (x + \xi^2)(x + \xi^6) \in \mathbb{F}_3(\xi)[x]$, we see that

$$A \cong \mathbb{F}_3(\xi)[x]/(x + \xi^2) \oplus \mathbb{F}_3(\xi)[x]/(x + \xi^6) \cong \mathbb{F}_9 \oplus \mathbb{F}_9.$$

The automorphism group of A is the dihedral group D_4 of order 8 generated by the automorphism $\theta : A \to A; \xi \mapsto x + 2, x \mapsto \xi^6$ of order 4 and $\psi : A \to A; \xi \mapsto \xi, x \mapsto 2x$ of order 2. So, there are 5 automorphism of order 2: ψ, $\theta\psi$, $\theta^2\psi$, $\theta^3\psi$ and θ^2. Outside of the subgroups of order 2 generated by the elements of order 2, there are 3 proper subgroups, $Aut(A)$, $\langle\theta\rangle$, $\langle\psi, \theta^2\rangle$ and $\langle\theta\psi, \theta^2\rangle$ each of which is of order 4. Using Magma, we have found the number of σ-pseudo-self-dual bases of A over R with respect to H for each involution of A, each subgroup H of $Aut(A)$ and each subring R of A. The results are presented in Table 1. In the table, a gray highlighted involution σ indicates that $\sigma(R) = R$ and a gray highlighted subgroup H indicates that H fixes R element-wise (which, according to theorem 3.7, will insure a duality preserving basis for the corresponding Gray map Φ). Note that some bases will be found with multiple subgroups.

Example 3.5. Assume $A = GR(4, 2)$, the Galois ring consisting of all elements of the form $\beta_0 + \beta_1\xi$ where $\beta_i \in \mathbb{Z}_4$ and $\xi^2 + \xi + 1 = 0$. The automorphism group of A is of order 2 generated by $\theta : A \to A$ defined by $\theta : \xi \mapsto 3\xi + 3$. Assume $\sigma = \theta$, $\mathcal{B} = (\xi, \xi+3)$ and $H = Aut(A) = \{id, \theta\}$. Now, $Tr_H(\xi\sigma(\xi)) = 3$, $Tr_H(\xi\sigma(\xi+3)) = 0$, $Tr_H((\xi+3)\sigma(\xi)) = 0$ and $Tr_H((\xi+3)\sigma(\xi+3)) = 3$ showing that $\mathcal{B}$ is a σ-pseudo-self-dual basis where $\gamma = 3$. With a similar verification we see that if $\sigma = id$, $\mathcal{B}$ is a σ-pseudo-self-dual basis where $\gamma = 3$ as well. In [7], $\{\xi, \xi + 3\}$ was used to map Euclidean self-dual codes over A to Euclidean self-dual codes over $\mathbb{Z}_4$.

Using Magma we found that with $\sigma = id$ or $\sigma = \theta$, A has no σ-self-dual basis over its prime ring $\mathbb{Z}_4$, but has 8 σ-pseudo-self-dual bases over $\mathbb{Z}_4$:

$$\{3\xi + 2, \xi + 1\}, \{\xi + 1, \xi + 2\}, \{3\xi + 2, 3\xi + 3\}, \{3\xi + 1, \xi\}$$
$$\{3\xi + 3, \xi + 2\}, \{\xi, \xi + 3\}, \{3\xi, \xi + 3\}, \{3\xi, 3\xi + 1\}.$$

The previous examples show that σ-pseudo-self-dual bases have been used in the literature and also that even for small algebras they may be abundant. We soon give the main result of this subsection which shows that under a σ-pseudo-self-dual bases, the image of the dual of a code is the dual of the image i.e. preserves duality given some additional conditions. The first condition is that $\sigma(R) = R$ which we have already imposed throughout this section. This is to guarantee that the σ hermitian form on A restricts to a hermitian form on R. The second condition is that $R \subset A^H$. The next example shows that with out this, a σ-pseudo-self-dual basis does not necessarily preserve duality.

Example 3.6. We continue in the setting of Example 3.4. Assume $R = \mathbb{F}_3(\xi)$ and $\sigma = \psi$ (notice $\psi(\mathbb{F}_3(\xi)) = \mathbb{F}_3(\xi)$). Assume $\mathcal{B} = \{1, \xi^2x+\xi^2\}$. The R-basis of A, $\mathcal{B}$, is a σ-pseudo-self-dual basis with respect to $Aut(A)$. Notice $R \not\subset A^{Aut(A)}$. Let C be the $[2, 1]$ linear code over A generated by

$$\begin{pmatrix} 1 & \xi^2x \end{pmatrix}$$

which is a σ-hermitian self-dual code over A. The code $\Phi(C)$, whose generator matrix is,

$$\begin{pmatrix} 1 & 0 & \xi^6 & 1 \\ 0 & 1 & 2 & \xi^2 \end{pmatrix}$$

is not a euclidian self-dual code over R.

The next theorem is the first of our two main theorems, each of which provides conditions for mapping the dual of a code over A to the dual of its image over R.

Theorem 3.7. *Let H be a subgroup of the automorphism group of A such that $R \subset A^H$ and let C be an n length linear code over A. Assume $\mathcal{B}$ is σ-pseudo-self-dual basis w.r.t H. Then*

$$\Phi(C^\perp) \subset \Phi(C)^\perp.$$

Furthermore, if A and R are Frobenius rings then

$$\Phi(C^\perp) = \Phi(C)^\perp.$$

Proof. Since $\mathcal{B}$ is σ-pseudo-self-dual basis w.r.t H there exists a $\gamma \in A$ that commutes with R, is not a zero divisor and for $1 \leq i, j \leq r$ with $i \neq j$, $Tr_H(v_i\sigma(v_i)) = \gamma$ and $Tr_H(v_i\sigma(v_j)) = 0$. Let $x = (x_1, \ldots, x_n) \in A^n$ and $y = (y_1, \ldots, y_n) \in A^n$ where $x_i = \sum_{j=1}^r \alpha_{ij} v_j \in A$ and $y_i = \sum_{k=1}^r \beta_{ik} v_k \in A$. Assume $\langle x, y \rangle_{A^n} = 0$. Since $R \subset A^H$, by Lemma 2.1 we have that

$$\begin{aligned}
0 &= Tr_H(0) = Tr_H(\langle x, y \rangle_{A^n}) = Tr_H\left(\sum_{i=1}^n \left(\sum_{j=1}^r \alpha_{ij} v_j\right) \sigma\left(\sum_{k=1}^r \beta_{ik} v_k\right)\right) \\
&= Tr_H\left(\sum_{i=1}^n \left(\sum_{j=1}^r \alpha_{ij} v_j\right)\left(\sum_{k=1}^r \sigma(v_k)\,\sigma(\beta_{ik})\right)\right) \\
&= \sum_{i=1}^n \sum_{j=1}^r \sum_{k=1}^r \alpha_{ij} Tr_H(v_j \sigma(v_k))\,\sigma(\beta_{ik}) = \sum_{i=1}^n \sum_{j=1}^r \alpha_{ij} Tr_H(v_j \sigma(v_j))\,\sigma(\beta_{ij}) \\
&= \sum_{i=1}^n \sum_{j=1}^r \alpha_{ij} \gamma \sigma(\beta_{ij}) = \gamma \sum_{i=1}^n \sum_{j=1}^r \alpha_{ij} \sigma(\beta_{ij}) \\
&= \gamma \langle \Phi(x), \Phi(y) \rangle_{R^{nr}}.
\end{aligned}$$

Since γ is not a zero divisor, $\langle \Phi(x), \Phi(y) \rangle_{R^{nr}} = 0$. With this it is easy to see that $\Phi(C^\perp) \subset \Phi(C)^\perp$.

Now, $|C| = |\Phi(C)|$. Since A and R are Frobenius rings, from Lemma 2.3, we have that

$$|C^\perp| = \frac{|A|^n}{|C|} = \frac{|R|^{rn}}{|\Phi(C)|} = |\Phi(C)^\perp|.$$

Hence, $\Phi(C^\perp) = \Phi(C)^\perp$. □

For an alternate view of the previous result, we return to the notation introduced at the beginning of this section. From Lemma 3.2 we have that

$$\langle x, y\rangle_{A^n} = \Phi(x)\mathcal{M}\sigma(\Phi(y))^T.$$

In the setting of Theorem 3.7 we have then

$$\begin{aligned} 0 &= Tr_H(0) = Tr_H(\langle x, y\rangle_{A^n}) = Tr_H(\Phi(x)\mathcal{M}\sigma(\Phi(y)^T)) \\ &= \Phi(x)Tr_H(\mathcal{M})\sigma(\Phi(y)^T) = \Phi(x)\gamma I_{nr}\sigma(\Phi(y)^T) = \gamma\langle\Phi(x), \Phi(y)\rangle_{R^{nr}}. \end{aligned}$$

Again, since γ is not a zero divisor, $\langle\Phi(x), \Phi(y)\rangle_{R^{nr}} = 0$. The point here is this. In general, if $Tr_H(\mathcal{M}) = \gamma I_{nr}$ which boils down to $Tr_H(M) = \gamma I_r$, then $\mathcal{B}$ is a σ-pseudo-self-dual basis for A over R. If in addition, $R \subset A^H$, $\mathcal{B}$ will preserve duality.

Example 3.8. We again continue in the setting of Examples 3.4 and 3.6. Remember $A = \mathbb{F}_3(\xi)[x]/(x^2 + 1)$ where $\xi^2 + 2\xi + 2 = 0$, $R = \mathbb{F}_3(\xi)$ and $\sigma : A \to A; \xi \mapsto \xi, x \mapsto 2x$. Here we assume $\mathcal{B} = \{1, x\}$. As in Example 3.6, the basis here is a σ-pseudo-self-dual basis but it is with respect to $\langle\sigma\rangle \subset Aut(A)$. What is different is that R is in the fixed ring of the subgroup i.e. $R \subset A^{\langle\sigma\rangle}$. Remember, the code C generated by

$$\begin{pmatrix} 1 & \xi^2 x \end{pmatrix}$$

is a σ-hermitian self-dual code. With the redefinition of $\mathcal{B}$, the code $\Phi(C)$, will have generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & \xi^2 \\ 0 & 1 & \xi^6 & 0 \end{pmatrix}.$$

But, unlike the image of this code in Example 3.6, the image here is a euclidian self-dual code over A.

It is not always the case that A has a σ-pseudo-self-dual basis over R. For instance, from the full list of indecomposable commutative rings of order 16 given in [14], none of the rings $\mathbb{F}_4[x]/(x^2)$, $\mathbb{F}_2[x]/(x^2 + y^2, xy)$, $\mathbb{F}_2[x]/(x^2, y^2)$, $\mathbb{Z}_4[x]/(x^2 + 2x)$, $\mathbb{Z}_4[x]/(x^2 + 2)$, $\mathbb{Z}_4[x]/(x^2 + 2x + 2)$ and $\mathbb{Z}_4[x]/(x^2)$ have a σ-pseudo-self-dual basis for any proper subring. This is not to say that no duality preserving map exists over these rings as will be seen in the next subsection where we look at an alternative property which guarantees duality preservation. In the case of $\mathbb{Z}_4[x]/(x^2)$ it is true that no such duality preserving map exists as this was shown in [15]. Similarly, we can find examples where A is non-commutative and does not have a σ-pseudo-self-dual basis over R. For instance, $\frac{\mathbb{F}_4[x;\theta]}{\langle x^2\rangle}$ where θ is the Frobenius map on $\mathbb{F}_4$ extended to $\frac{\mathbb{F}_4[x;\theta]}{\langle x^2\rangle}$.

The next two results have to do with scaling σ-pseudo-self-dual bases in order to obtain other σ-pseudo-self-dual bases. In Proposition 3.9, given a σ-pseudo-self-dual basis, another σ-pseudo-self-dual basis was found. In Proposition 3.10, given an involution φ on A and a σ-pseudo-self-dual basis, a $\varphi\sigma\varphi$-pseudo-self-dual basis is found i.e. the new basis is pseudo-self-dual for the $\varphi\sigma\varphi$ sesquilinear form.

Proposition 3.9. *Let H be a subgroup of the automorphism group of A and $a \in A^H$ such that $\sigma(a) \in A^H$, that is not a zero divisor and commutes with the elements of R. Assume $\{v_1, \ldots, v_n\}$ is σ-pseudo-self-dual basis with respect to H where for some $\gamma \in A^H$, $Tr_H(v_i\sigma(v_i)) = \gamma$. Then $\{av_1, \ldots, av_n\}$ is a σ-pseudo-self-dual basis for $\gamma' = a\gamma\sigma(a)$ with respect to H.*

Proof. Since $a, \sigma(a) \in A^H$, by Lemma 2.1 we have that

$$\begin{aligned} Tr_H(v_i\sigma(v_i)) &= \gamma \\ aTr_H(v_i\sigma(v_i))\sigma(a) &= a\gamma\sigma(a) \\ Tr_H(av_i\sigma(v_i)\sigma(a)) &= a\gamma\sigma(a) \\ Tr_H(av_i\sigma(av_i)) &= a\gamma\sigma(a). \end{aligned}$$

Since a is regular, so is $\sigma(a)$ and $a\gamma\sigma(a)$. The result follows. □

Proposition 3.10. *Let H be a subgroup of $Aut(A)$ and φ be an involution on A. Denote by θ, the automorphism $\varphi\sigma$ of A, by $\widehat{\sigma}$, the involution $\varphi\sigma\varphi$ of A, by $\widehat{H}$ the subgroup $\varphi H\varphi$ of $\mathrm{Aut}(A)$ and by $\widehat{\mathcal{B}}$, the $\theta(R)$-basis of A, $\{\theta(v_1), \ldots, \theta(v_n)\}$. Then*

1. *For $\widehat{v} = \theta(v)$ and $\widehat{w} = \theta(w)$ in $\widehat{\mathcal{B}}$, $Tr_{\widehat{H}}(\widehat{v}\sigma(\widehat{w})) = \varphi\left(Tr_H(w\sigma(v))\right)$.*
2. *If $\mathcal{B}$ is σ-pseudo-self-dual basis w.r.t H over R of A then $\widehat{\mathcal{B}}$ is a $\widehat{\sigma}$-pseudo-self-dual basis w.r.t $\widehat{H}$ over $\theta(R)$ of A.*

Proof. The first statement follows by a simple computation:

$$\begin{aligned} Tr_{\widehat{H}}(\widehat{v}\sigma(\widehat{w})) &= \sum_{h\in\widehat{H}} h(\widehat{v}\widehat{\sigma}(\widehat{w}) = \sum_{h\in H} \varphi h\varphi(\varphi\sigma(v)\varphi\sigma\varphi(\varphi\sigma(w)) \\ &= \varphi \sum_{h\in H} h(w\sigma(v)) = \varphi\left(Tr_H(w\sigma(v))\right). \end{aligned}$$

For the second statement one verifies that $\widehat{\mathcal{B}}$ is a left $\theta(R)$-basis of A. Suppose that $\mathcal{B}$ is σ-pseudo-self-dual basis w.r.t H for $\gamma = (Tr_H(v_i\sigma(v_i)))$, where γ is not a zero divisor that commutes with the elements of R. From the first statement we obtain for $1 \leq i, j \leq r$ that $Tr_{\widehat{H}}(\theta(v_i)\sigma(\theta(v_j))) = 0$ if $i \neq j$ and $Tr_{\widehat{H}}(\theta(v_i)\sigma(\theta(v_i))) = \varphi(\gamma)$. Since γ is not a zero divisor, $\varphi(\gamma)$ is not a zero divisor and it only remains to show that $\varphi(\gamma)$ commutes with elements of $\varphi(R)$. For $r \in R$, since $\sigma(R) = R$ and γ commutes with elements of R,

$$\varphi(\gamma)\theta(r) = \varphi(\gamma)\varphi(\sigma(r)) = \varphi(\sigma(r)\gamma) = \varphi(\gamma\sigma(r)) = \varphi(\sigma(r))\varphi(\gamma) = \theta(r)\varphi(\gamma)$$

and the result follows. □

Example 3.11. In Table 1, the table associated with Example 3.4, we see that starting with the table for $R = \mathbb{F}_3(\xi)$, swapping rows 2 and 4 and then

columns 1 and 3 we end up with the table for $R = \mathbb{F}_3(x+1)$. This can be explained using Proposition 3.10. Notice that the number of ψ-pseudo-self-dual bases with respect to $\langle\theta^2\psi\rangle$ of A over $\mathbb{F}_3(\xi)$ is 64. Now, $(\theta\psi)\psi(\theta\psi) = \theta^2\psi$, $(\theta\psi)\langle\theta^2\psi\rangle(\theta\psi) = \langle\psi\rangle$ and $(\theta\psi)\psi = \theta$. Since $\theta(\mathbb{F}_3(\xi)) = \mathbb{F}_3(x+1)$, Proposition 3.10 shows that there are 64 $\theta^2\psi$-pseudo-self-dual bases with respect to $\langle\psi\rangle$ of A over $\mathbb{F}_3(x+1)$.

Example 3.12. In Example A.1, a full analysis is given of σ-pseudo-self-dual bases on $M_2(\mathbb{F}_2)$. Here we refer to that example. Since ψ conjugated with any involution is ψ, applying Proposition 3.10 to a ψ-pseudo-self-dual basis will produce a ψ-pseudo-self-dual basis. Similarly, τ conjugated with τ or ψ is τ, applying Proposition 3.10 in these cases will only produce a τ-pseudo-self-dual basis from τ-pseudo-self-dual basis. More interestingly though, $(\tau\theta)\tau(\tau\theta) = \tau\theta^2$. Now if we apply Proposition 3.10 with the involution $\tau\theta$ to a τ-pseudo-self-dual basis, we obtain a $\tau\theta^2$-pseudo-self-dual basis. Similarly, $(\tau\theta^2)\tau(\tau\theta^2) = \tau\theta$. If we apply Proposition 3.10 with the involution $\tau\theta^2$ to a τ-pseudo-self-dual basis, we obtain a $\tau\theta$-pseudo-self-dual basis. This explains why there are the same number of τ, $\tau\theta$ and $\tau\theta^2$ pseudo-self-dual bases.

3.2 Symmetric Bases

In this section assume additionally that A is a free R-algebra not simply a left R-module. Although we do not assume A is commutative here, if we assume the R basis $\mathcal{B}$ to be symmetric (defined below), then A must be commutative. See Lemma 3.15. So, this section in reality is strictly about commutative alphabets. In the commutative case, σ is simply an order two automorphism or the identity map. This allows us to consider the Euclidean inner product on commutative rings in our setting which is not possible in the non-commutative case as the identity map is not an involution in that case.

In [16], symmetric bases were defined for field extensions. As we did with trace orthogonal bases in the last section, we extend the definition of symmetric bases to include the ring extensions we are considering.

Definition 3.13. For $a \in A$, let M_a denote the matrix w.r.t. $\mathcal{B}$ representing the linear transformation of right multiplication by a, i.e.

$$M_a = \begin{bmatrix} \rho(v_1 a) \\ \vdots \\ \rho(v_r a) \end{bmatrix}.$$

We say $\mathcal{B}$ is a *symmetric basis* if for any $v \in \mathcal{B}$, $M_v = M_v^T$.

Example 3.14. Assume $A = \mathbb{F}_2(\xi)[x]/(x^2)$ where $\xi^2 + \xi + 1 = 0$ ($\mathbb{F}_2(\xi) \cong \mathbb{F}_4$) and $\mathcal{B} = (1, \xi x + 1)$ which is an $\mathbb{F}_2(\xi)$-basis for A. See [13] for specific work on codes over $\mathbb{F}_4[x]/(x^2)$. Using the embedding described in Definition 3.13, we have $M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $M_{x+1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ showing that $\mathcal{B}$ is symmetric.

In the above definition M_a acts on row vectors from R^r on the right. It is well know that sending $a \in A$ to M_a is an embedding of A in $M_r(R)$. Before getting to the main result of the section, we have a lemma with a few simple results needed throughout. The most important of these is that for A to have a symmetric basis, it must be commutative.

Lemma 3.15. *1. For $a, b \in A$, $\rho(ab) = \rho(a)M_b$ and $ab = \rho^{-1}(\rho(a)M_b)$.*

2. If $\mathcal{B}$ is symmetric, then for $a \in A$, $M_a = M_a^T$ and A is commutative.

Proof. Let $a, b \in A$. Since $\rho(a)$ is just the representation of a in $\mathcal{B}$, $\rho(ab) = \rho(a)M_b$ and $ab = \rho^{-1}(\rho(a)M_b)$. If $\mathcal{B}$ is symmetric, since $\{M_v | v \in \mathcal{B}\}$ is a basis for $\{M_a | a \in A\}$ we have that $M_a = M_a^T$ and so

$$M_{ab} = M_a M_b = (M_a M_b)^T = M_b^T M_a^T = M_b M_a = M_{ba}.$$

Finally, $ab = ba$. □

As was the case with pseudo-self-dual bases, symmetric bases also preserve duality given an additional condition which is the main result of this section. In addition to a basis being symmetric, for the basis to guarantee duality preservation, σ must fix the basis element-wise.

Example 3.16. Continuing with Example 3.14 where $A = F_2(\xi)[x]/(x^2)$ and $\mathcal{B} = (1, \xi x + 1)$, assume σ is the Frobenius map on $\mathbb{F}_2(\xi)$ extended linearly to A. Remember, $\mathcal{B}$ is symmetric and observe that $\sigma(1) = 1$ and $\sigma(\xi x + 1) = \xi^2 x + 1$ meaning σ does not fix $\mathcal{B}$ element-wise. Let C be the $[2, 1]$ linear code over A generated by

$$\begin{pmatrix} 1 & 1 + x \end{pmatrix}$$

which is a σ-hermitian self-dual code over A. The code $\Phi(C)$, whose generator matrix is,

$$\begin{pmatrix} 1 & 0 & \xi & \xi^2 \\ 0 & 1 & \xi^2 & \xi \end{pmatrix}$$

is not a σ-hermitian self-dual code over $\mathbb{F}_2(\xi)$.

This next theorem, the second of our two main results, shows that if a basis is symmetric and is fixed by σ element-wise, the basis preserves duality.

Theorem 3.17. *Let C be an n length linear code over A. Assume $\mathcal{B}$ is symmetric and σ fixes the elements of $\mathcal{B}$. Then*

$$\Phi(C^\perp) \subset \Phi(C)^\perp.$$

Furthermore, if A and R are Frobenius rings then

$$\Phi(C^\perp) = \Phi(C)^\perp.$$

Proof. Let $a = \alpha_1 v_1 + \cdots + \alpha_r v_r, b = \beta_1 v_1 + \cdots + \beta_r v_r \in A$ where $\alpha_i, \beta_i \in R$. Since σ fixes the elements of $\mathcal{B}$, $(\sigma(\beta_1), \ldots, \sigma(\beta_r)) = \rho(\sigma(b)) = \rho(1)M_{\sigma(b)}$. So,

$$\langle \rho(a), \rho(b) \rangle_{R^r} = \sum_{i=1}^{r} \alpha_i \sigma(\beta_i) = \rho(1) M_a \left(\rho(1) M_{\sigma(b)}\right)^T.$$

Since $\langle a, b \rangle = 0$, $0 = \sum_{i=1}^{n} \alpha_i \sigma(\beta_i)$ which implies $0 = \sum_{i=1}^{n} M_{\alpha_i} M_{\sigma(\beta_i)}$. Since $\mathcal{B}$ is symmetric, by Lemma 3.15 we have

$$\begin{aligned} \langle \Phi(a), \Phi(b) \rangle_{R^{nr}} &= \sum_{i=1}^{n} \langle \rho(\alpha_i), \rho(\beta_i) \rangle_{R^r} = \sum_{i=1}^{n} \rho(1) M_{\alpha_i} \left(\rho(1) M_{\sigma(\beta_i)}\right)^T \\ &= \sum_{i=1}^{n} \rho(1) M_{\alpha_i} M_{\sigma(\beta_i)}^T \rho(1)^T \\ &= \rho(1) \left(\sum_{i=1}^{n} M_{\alpha_i} M_{\sigma(\beta_i)} \right) \rho(1)^T = 0. \end{aligned}$$

This shows that $\Phi(C^\perp) \subset \Phi(C)^\perp$. We know $|C| = |\Phi(C)|$. Since A and R are Frobenius rings, from Lemma 2.3, we have that

$$|C^\perp| = \frac{|A|^n}{|C|} = \frac{|R|^{rn}}{|\Phi(C)|} = |\Phi(C)^\perp|.$$

□

Example 3.18. As in Example 3.16 assume $A = \mathbb{F}_2(\xi)[x]/(x^2)$ and σ is the Frobenius map on $\mathbb{F}_4$ extended linearly to A. But, here assume $\mathcal{B} = (1, x+1)$. It is easy to check that $\mathcal{B}$ is symmetric but unlike the basis in Example 3.16, σ fixes $\mathcal{B}$ element-wise. We again consider the code C generated by

$$\begin{pmatrix} 1 & 1+x \end{pmatrix}$$

which is a σ-hermitian self-dual code over A. The code $\Phi(C)$, whose generator matrix is,

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

is a σ-hermitian self-dual code over $\mathbb{F}_2(\xi)$. This was expected due to Theorem 3.17.

Using Magma, we determined that there are no pseudo-self-dual bases for $\mathbb{F}_2(\xi)[x]/(x^2)$ over $\mathbb{F}_2(\xi)$ nor $\mathbb{F}_2$. As we have seen there are however symmetric bases over $\mathbb{F}_2(\xi)$. The next Example shows the abundance of symmetric bases of $\mathbb{F}_2(\xi)$ over its various subrings.

Example 3.19. Assume $A = \mathbb{F}_2(\xi)[x]/(x^2)$ where $\xi^2 + \xi + 1 = 0$. A has 18 symmetric bases over $\mathbb{F}_2(\xi)$ (out of 90 bases over $\mathbb{F}_2(\xi)$):

$$\{1, x+1\}, \{\xi, \xi(x+1)\}, \{\xi^2, \xi^2(x+1)\}$$

$$\{1, \xi x + 1\}, \{\xi, \xi^2 x + \xi)\}, \{\xi^2, x + \xi^2)\}$$
$$\{1, \xi^2 x + 1\}, \{\xi, x + \xi)\}, \{\xi^2, \xi x + \xi^2)\}$$
$$\{x + 1, \xi x + 1\}, \{\xi(x + 1), \xi^2 x + \xi\}, \{\xi^2(x + 1), x + \xi^2\}$$
$$\{x + 1, \xi^2 x + 1\}, \{\xi(x + 1), x + \xi\}, \{\xi^2(x + 1), \xi x + \xi^2\}$$
$$\{x + \xi, \xi^2 x + \xi\}, \{\xi x + \xi^2, x + \xi^2\}, \{\xi^2 x + 1, \xi x + 1\}$$

1. If σ is the identity map, any of these symmetric bases will preserve duality. The inner product restricts to the Euclidean inner product on $\mathbb{F}_2(\xi)$.
2. If σ is defined by $\xi \mapsto \xi^2$ and $x \mapsto x$, the unique symmetric basis that is fixed by σ is $\{1, x+1\}$ meaning it is the only basis that preserves duality. The inner product restricts to the hermitian inner product on $\mathbb{F}_2(\xi)$.
3. If σ is defined by $\xi \mapsto \xi^2$ and $x \mapsto \xi x$, the unique symmetric basis that is fixed by σ is $\{1, \xi^2 x + 1\}$ meaning it is the only basis that preserves duality. The inner product restricts to the hermitian inner product on $\mathbb{F}_2(\xi)$.
4. If σ is defined by $\xi \mapsto \xi^2$ and $x \mapsto \xi^2 x$, the unique symmetric basis that is fixed by σ is $\{1, \xi x+1\}$ meaning it is the only basis that preserves duality. The inner product restricts to the hermitian inner product on $\mathbb{F}_2(\xi)$.

The ring A has also 18 symmetric bases over $\mathbb{F}_2$ (out of 840 bases of A over $\mathbb{F}_2$). Since only the identity map can fix the elements of a basis over the prime ring, for any involution of order 2, none of these bases are duality preserving.

The ring A has also 3 subrings isomorphic to $\mathbb{F}_2[x]/(x^2)$ (in some coding theory papers denoted as $\mathbb{F}_2 + u\mathbb{F}_2$), one of them is $R = \mathbb{F}_2[x]/(x^2) \subset \mathbb{F}_4[x]/(x^2)$. There are 24 symmetric bases of A over R, one such basis is $(1, \xi)$ and

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } M_\xi = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Another symmetric basis of A over R is $(x + 1, \xi)$ and

$$M_{x+1} = \begin{pmatrix} x+1 & 0 \\ 0 & x+1 \end{pmatrix} \text{ and } M_\xi = \begin{pmatrix} 0 & x+1 \\ x+1 & 1 \end{pmatrix}.$$

To finish this section, we study specifically $\mathbb{F}_q[x]/(x^t)$ which was considered in [2]. Among other results, a condition on the change of basis matrix which changes from the standard basis, $\{1, x, \ldots, x^{t-1}\}$, to some other basis is given which guarantees that the new basis preserves orthogonality. It turns out that this condition is equivalent to the new basis being symmetric. This is the subject of the next proposition.

Proposition 3.20. *Assume $A = \mathbb{F}_q[x]/(x^r)$ and $R = \mathbb{F}_q$. Let B be a change of basis matrix from the standard $\mathbb{F}_q$-basis for A to the $\mathbb{F}_q$-basis $\mathcal{B}$. Then the following are equivalent:*

1. *$\mathcal{B}$ is symmetric.*

2. *BB^T is upper anti-triangular with constant anti-diagonal as well as all parallel diagonals (i.e. for $b_{ij} = \left(BB^T\right)_{ij}$, if $i + j > r + 1$ then $b_{ij} = 0$ and if $k = i + j \leq r + 1$, $b_{1,k-1} = b_{2,k-2} \cdots = b_{k-1,1}$).*

Proof. In the following we use the embedding of A in $M_r(\mathbb{F}_q)$ as in Definition 3.13 where for $a \in A$, M_a is its matrix representation and $\cdot$ is the Euclidean inner product on $\mathbb{F}_q^r$ with respect to $\mathcal{B}$. Then $B^T = \left[\rho(1)^T, \rho(x)^T, \ldots, \rho(x^{r-1})^T\right]$, showing $\left(BB^T\right)_{ij} = \rho(x^{i-1}) \cdot \rho(x^{j-1})$.

Assume $\mathcal{B}$ is symmetric. Then for $m, n \geq 0$

$$\begin{aligned}
\rho(x^m) \cdot \rho(x^n) &= \rho(1)M_{x^m} \left(\rho(1)M_{x^n}\right)^T = \rho(1)M_{x^m}M_{x^n}^T\rho(1)^T \\
&= \rho(1)M_{x^m}M_{x^n}\rho(1)^T = \rho(1)M_1M_{x^{m+n}}\rho(1)^T \\
&= \rho(1)M_1M_{x^{m+n}}^T\rho(1)^T = \rho(1)M_1 \left(\rho(1)M_{x^{m+n}}\right)^T \\
&= \rho(1) \cdot \rho(x^{m+n}).
\end{aligned}$$

With this it can easily be shown BB^T is upper anti-triangular with constant anti-diagonals.

Now assume BB^T is upper triangular with constant anti-diagonals. This condition is equivalent to saying $\rho(1)\cdot\rho(x^k) = \rho(x)\cdot\rho(x^{k-1}) = \cdots = \rho(x^k)\cdot\rho(1)$. In some sense this says that the inner product respects the multiplication in A. Using this condition it can be shown that $\rho(ab)\cdot\rho(c) = \rho(a)\cdot\rho(bc)$ for $a, b, c \in A$. Let $a \in A$. Since $\left(M_aM_1^T\right)_{ij} = \rho(v_ia) \cdot \rho(v_j) = \rho(v_i) \cdot \rho(v_ja) = \left(M_1M_a^T\right)_{ij}$ we have that $M_a = M_aM_1 = M_aM_1^T = M_1M_a^T = M_a^T$. Hence, $\mathcal{B}$ is symmetric. □

Now that we see that the condition presented in [2] Proposition 5 is equivalent to a basis being symmetric, it is clear that their condition guarantees that the basis preserves duality which is the essence of Proposition 5 and Corollary 1 in [2].

4 Examples using cyclic self-dual codes

We give some examples of rings and bases which show that the best minimum Gray weight obtained for a family of self-dual codes depends of the choice of the basis for which the Gray weight is with respect to. From this it can be concluded that, for a given problem, not all bases share the same properties and that some care has to be taken when choosing a basis.

A cyclic code C over a finite commutative ring A is an ideal $(g)/(Y^n - 1) \subset A[Y]/(Y^n - 1)$, where the polynomial $g = g_0 + \ldots + g_{n-k-1}Y^{n-k-1} + g_{n-k}Y^{n-k}$ is a divisor of $Y^n - 1 \in A[Y]$. The generating matrix of the corresponding linear

code is

$$G = \begin{pmatrix} g_0 & \dots & g_{n-k-1} & g_{n-k} & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{n-k-1} & g_{n-k} & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \dots & 0 & g_0 & \dots & g_{n-k-1} & g_{n-k} \end{pmatrix}.$$

If $h_0 \in A$ is invertible, then the reciprocal polynomial of $h = \sum_{i=0}^{r} h_i Y^i \in A[Y]$ is $h^* = \frac{1}{h_0} \sum_{i=0}^{r} h_{r-i} Y^i$. For an automorphism σ of order 2 we also define $h^*_\sigma = \frac{1}{\sigma(h_0)} \sum_{i=0}^{r} \sigma(h_{r-i}) Y^i$. It is well known that the cyclic code $(g)/(Y^n-1) \subset A[Y]/(Y^n-1)$ is euclidian self-dual if and only if $Y^n - 1 = h \cdot g$ and $g = h^*$ and is σ-hermitian self-dual if and only if $Y^n - 1 = h \cdot g$ and $g = h^*_\sigma$.

Row $i+1$ of the above generator matrix of C corresponds to the polynomials $Y^i g$. If A is a free R-module for some subring R of A, then for an R-basis of A, $\{v_1, \dots, v_r\}$, C is spanned over R by

$$v_1 g, \cdots, v_r g, v_1 Y g, \cdots, v_r Y g, \cdots, v_1 Y^k g, \cdots, v_r Y^k g.$$

Therefore the lines of a generator matrix of $\Phi(C)$ are given by the image under Φ of the vectors corresponding to these polynomials.

4.1 Euclidean self-dual cyclic codes over $\mathbb{F}_4[x]/(x^3)$

Denote $A = \mathbb{F}_4[x]/(x^3)$ and $\mathbb{F}_4 = \mathbb{F}_2(\xi)$. We obtain the following decompositions in $A[Y]$ (which is not a unique factorization domain)

$$\begin{aligned} Y^2 - 1 &= (Y+1)(Y+1) \\ &= (Y + x^2 + 1)(Y + x^2 + 1) \\ &= (Y + \xi x^2 + 1)(Y + \xi x^2 + 1) \\ &= (Y + \xi^2 x^2 + 1)(Y + \xi^2 x^2 + 1) \end{aligned}$$

where each constant term is its own inverse. Therefore there exists four self-dual cyclic codes $(g)/(Y^2-1) \subset A[Y]/(Y^2-1)$ over A, generated by $g_1 = Y + 1$, $g_2 = Y + x^2 + 1$, $g_3 = Y + \xi x^2 + 1$ and $g_4 = Y + \xi^2 x^2 + 1$. In order to map those self-dual codes over A to self dual codes over $\mathbb{F}_4$ we verified the symmetric basis criteria for all 30240 $\mathbb{F}_4$-bases of A and found 480 distinct symmetric bases. Also, there are no (pseudo)-self-dual bases over $\mathbb{F}_4$. We consider the following two symmetric bases of A over $R = \mathbb{F}_4$.

$$\mathcal{B}_1 = [\xi^2 x + 1,\, \xi x,\, \xi^2 x^2 + \xi^2 x + 1];\ \mathcal{B}_2 = [\xi^2 x^2 + \xi^2, x^2 + \xi^2 x + \xi, \xi^2 x^2 + x + 1]$$

1. Using the basis $\mathcal{B}_1$ we obtain that the image codes over $\mathbb{F}_4$ of the self dual codes $(g)/(Y^2-1) \subset A[Y]/(Y^2-1)$ over A has the following generator matrix (Here the lines of the generator matrix corresponds to the coefficients of $(\xi^2 x + 1) \cdot g, (\xi x) \cdot g$ and $(\xi^2 x^2 + \xi^2 x + 1) \cdot g$ in the basis $\mathcal{B}_1$) and weight enumerator:

- g_1: $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$ and $1 + 9w^2 + 27w^4 + 27w^6$.
- g_2: $\begin{pmatrix} \xi^2 & 0 & \xi & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ \xi & 0 & \xi^2 & 0 & 0 & 1 \end{pmatrix}$ and $1+3w^2+12w^3+3w^4+36w^5+9w^6$
- g_3: $\begin{pmatrix} \xi & 0 & \xi^2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ \xi^2 & 0 & \xi & 0 & 0 & 1 \end{pmatrix}$ and $1+3w^2+12w^3+3w^4+36w^5+9w^6$
- g_4: $\begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$ and $1 + 9w^2 + 27w^4 + 27w^6$

2. Using the basis $\mathcal{B}_2$ we obtain that the image codes over $\mathbb{F}_4$ of the self dual codes $(g)/(Y^2-1) \subset A[Y]/(Y^2-1)$ over A has the following generator matrix and weight enumerator:

   - g_1 : we obtain the same code $\Phi(C)$ as for $\mathcal{B}_1$.
   - g_2: $\begin{pmatrix} \xi & \xi & 1 & 1 & 0 & 0 \\ \xi & 0 & \xi^2 & 0 & 1 & 0 \\ 1 & \xi^2 & \xi^2 & 0 & 0 & 1 \end{pmatrix}$ and $1 + 6w^3 + 27w^4 + 18w^5 + 12w^6$
   - g_3: $\begin{pmatrix} 0 & \xi^2 & \xi & 1 & 0 & 0 \\ \xi^2 & \xi^2 & 1 & 0 & 1 & 0 \\ \xi & 1 & \xi & 0 & 0 & 1 \end{pmatrix}$ and $1 + 6w^3 + 27w^4 + 18w^5 + 12w^6$
   - g_4: $\begin{pmatrix} \xi^2 & 1 & \xi^2 & 1 & 0 & 0 \\ 1 & \xi & \xi & 0 & 1 & 0 \\ \xi^2 & \xi & 0 & 0 & 0 & 1 \end{pmatrix}$ and $1 + 6w^3 + 27w^4 + 18w^5 + 12w^6$

Using the first basis we would not have obtained a self-dual code over $\mathbb{F}_4$ of optimal hamming weight 3 (cf. [10]).

4.2 Hermitian self-dual cyclic codes over $\mathbb{F}_9[x]/(x^2-2)$

Consider the ring $A = \mathbb{F}_3(\xi)[x]/(x^2+1)$ where $\xi^2 + 2\xi + 2 = 0$ from Example 3.4. We obtain two factorizations of $Y^2 - 1$ in $A[Y]$ (which is not a unique factorization domain since $A \cong \mathbb{F}_9 \oplus \mathbb{F}_9$):

$$Y^2 - 1 = (Y + \xi^6 x)(Y + \xi^2 x) = (Y+1)(Y+2).$$

Each factor produces a $[2,1]$ cyclic code over A none of which are Euclidian self-dual codes nor θ^2-hermitian self-dual codes. However, the codes generated by the factors $Y + \xi^2 x$ and $Y + \xi^6 x$ generate codes that are both ψ-hermitian self-dual and $\psi\theta^2$-hermitian self-dual.

- From the table in Example 3.4 we see there are 64 ψ-pseudo-self-dual bases with respect to the subgroup $\langle\psi\rangle$. Since $\langle\psi\rangle$ fixes $\mathbb{F}_3(\xi)$ element-wise, each one of the bases will preserve duality. So, by Theorem 3.7, the $\mathbb{F}_3(\xi)$ images of the codes generated by $Y+\xi^2 x$ and $Y+\xi^6 x$ will each be a hermitian self-dual code over $\mathbb{F}_3(\xi)$. The best hamming distance of any of these images is 2.

- From the table in Example 3.4 we see there are 96 $\theta^2\psi$-pseudo-self-dual bases with respect to the subgroup $\langle\psi\rangle$. Since $\langle\psi\rangle$ fixes $\mathbb{F}_3(\xi)$ element-wise, each one of the bases will preserve duality. So, by Theorem 3.7, the $\mathbb{F}_3(\xi)$ images of the codes generated by $g_1 = Y+\xi^2 x$ and $g_2 = Y+\xi^6 x$ will each be a hermitian self-dual code over $\mathbb{F}_3(\xi)$.

  1. For the basis $\mathcal{B}_1 = (\xi x, \xi^6)$ the generator matrix of the image of this codes are respectively

$$\begin{pmatrix} 0 & \xi & 1 & 0 \\ \xi^7 & 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & \xi^5 & 1 & 0 \\ \xi^3 & 0 & 0 & 1 \end{pmatrix}$$

     which are both of hamming distance 2.

  2. For the basis $\mathcal{B}_2 = (2x+\xi^3, \xi^6 x+\xi)$ the generator matrix of the image of this codes are respectively

$$\begin{pmatrix} \xi^2 & \xi^2 & 1 & 0 \\ \xi^2 & \xi^6 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} \xi^6 & \xi^6 & 1 & 0 \\ \xi^6 & \xi^2 & 0 & 1 \end{pmatrix}$$

     which are both of hamming distance 3.

This illustrates that, the properties of all image codes of some family of self-dual codes C over A, can depend on the choice of the σ-pseudo-self-dual basis.

Acknowledgements

The first author would like to thank IRMAR for the support of his visit to their institution during which time this work was initiated.

A Pseudo-Self-Dual Bases of $M_2(\mathbb{F}_2)$

Example A.1. Let $A = M_2(\mathbb{F}_2)$. In [3], it was shown that codes over A can be mapped to codes over $\mathbb{F}_4$. In [1] self-dual cyclic codes over A were studied. In the process they show (Proposition 2 of [1]) that there is a map from A^n to $\mathbb{F}_4^{2n}$ that preserves self-orthogonality for a particular hermitian form. It turns out that this map is defined using a σ-self-dual $\mathbb{F}_4$ basis for A and the hermitian form is the standard σ-hermitian form on A where σ is the anti-transpose on A. Much more can be said about this map, specifically that it preserves duality for not only the hermitian form based on the anti-transpose on A but also the

hermitian form based on the transpose on A and a few others. This is what we shall show here. The following identifications for the elements of $M_2(\mathbb{F}_2)$ will be used throughout.

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},\ i = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ a = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$e_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},\ e_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},\ e_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},\ e_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$u_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix},\ u_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ u_3 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},\ u_4 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$$t = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix},\ b = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix},\ l = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix},\ r = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

We first compute the automorphisms and anti-automorphisms of A. The set of units of R is $\{I, i, u_1, u_2, u_3, u_4\}$. The units i, u_2 and u_3 are of multiplicative order 2 and the units u_1 and u_4 are of multiplicative order 3. The set $\{I, i, u_1, u_2\}$ is an F_2-basis for A. Replacing i or u_2 with u_3 will still be a basis, as will replacing u_1 with u_4. Now, any automorphism or anti-automorphism of A must send units to units of the same order. There are 12 such maps $A \to A$ that send units to units of the same order. They form a group isomorphic to a subgroup of S_6. Consider three of these maps which we express in cycle notation on the set of units. Let τ be the map (u_2u_3), ψ be the map(u_1u_5) and θ be the map (iu_2u_3). It turns out that τ is the transpose, ψ is the anti-transpose (the reflection of a matrix about the anti-diagonal) and

$$\theta : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} b+d & a+b+c+d \\ b & a+b \end{bmatrix}.$$

Note that τ and ψ are anti-automorphisms on A and θ is an automorphism on A. From this we deduce that the automorphism group is isomorphic to S_3 and generated by $\tau\psi$ and θ which is $\{id, \theta, \theta^2, \tau\psi, \tau\psi\theta, \tau\psi\theta^2\}$. The set of anti-isomorphisms are $\{\tau, \psi, \tau\theta, \psi\theta, \tau\theta^2, \psi\theta^2\}$. The subset of these, $\{\tau, \psi, \tau\theta, \tau\theta^2\}$, is the set of involutions of A, the remaining anti-isomorphisms having order 6.

Let $R = \{I, z, u_1, u_4\}$. Notice, R is a subring of A isomorphic to $\mathbb{F}_4$ and A is a free left R-module with left R-basis $\mathcal{B} = (I, i)$. Notice ψ is simply the Frobenius map when restricted to R and is the conjugation map on A from Section 4.2 in [1]. Of course $\psi(R) = R$. Let H be the group generated by θ whose fixed ring is R. Since $Tr_H(I\psi(i)) = Tr_H(i\psi(I)) = z$ and $Tr_H(I\psi(I)) = Tr_H(i\psi(i)) = I$, $\mathcal{B}$ is a ψ-self-dual basis w.r.t. H. Since A and R are Frobenius, by Theorem 3.7, the dual of a code over A is mapped to the dual of the image of the code over R where the hermitian form being considered is based on the anti-transpose. Since ψ restricted to R is simply the Frobenius map on $\mathbb{F}_4$ we are considering standard ψ-hermitian form on R.

It can be similarly shown that $\mathcal{B}$ is a τ-self-dual basis w.r.t. H. The difference here is that τ is the identity on R. So, the τ-hermitian form restricted to R is simply standard Euclidean form. Using Magma, we found all σ-pseudo-self-dual $\mathbb{F}_4$-bases and $\mathbb{F}_2$-bases for $M_2(\mathbb{F}_2)$ for each given involution, σ.

1. These are the σ-pseudo-self-dual $\mathbb{F}_4$-bases w.r.t. $H = \langle\theta\rangle$ for $M_2(\mathbb{F}_2)$ for each involution σ:
   - $\sigma = \psi$: $\{I, i\}, \{I, u_2\}, \{I, u_3\}, \{i, u_1\}, \{i, u_4\}, \{u_1, u_2\}, \{u_1, u_3\}, \{u_2, u_4\}, \{u_3, u_4\}$
   - $\sigma = \tau$: $\{I, i\}, \{e_1, e_2\}, \{l, r\}, \{e_3, e_4\}, \{u_1, u_2\}, \{u_3, u_4\}$.
   - $\sigma = \tau\theta$: $\{I, u_2\}, \{i, t\}, \{u_1, u_3\}, \{r, a\}, \{b, e_4\}, \{e_2, t\}$
   - $\sigma = \tau\theta^2$: $\{I, i\}, \{u_1, u_2\}, \{u_3, u_4\}, \{e_1, e_2\}, \{e_3, e_4\}$
2. The following are the σ-pseudo-self-dual $\mathbb{F}_2$-bases w.r.t. $H = Aut(A)$ for A for each involution σ :
   - $\sigma = \psi$: none
     $\sigma = \tau$: $\{u_1, u_2, u_3, u_4\}, \{e_1, e_2, e_3, e_4\}$
   - $\sigma = \tau\theta$: $\{i, u_1, u_3, u_4\}, \{r, a, e_2, t\}$
   - $\sigma = \tau\theta^2$: $\{i, u_1, u_2, u_4\}, \{r, a, b, e_3\}$

B Examples of Symmetric Bases

Example B.1. The Galois ring $A = GR(4, 2)$ defined in example **??** has 24 symmetric bases (among which are the 8 σ-pseudo-self-dual bases previously found). An example of a new basis is $\{1, \xi + 2\}$.

Example B.2. The ring $\mathbb{Z}_4[x]/(x^2 - 2x)$ (see [15]) has 16 symmetric basis. An example of such a basis is $\{1, x + 1\}$.

Example B.3. The ring $\mathbb{Z}_4[x]/(x^2 - 2)$ has 16 symmetric bases. An example of such a basis is $\{1, x + 1\}$.

Example B.4. The ring $\mathbb{Z}_4[x]/(x^2 - x)$ ([11]) has no σ-pseudo-self-dual bases, but has 8 symmetric bases over $\mathbb{Z}_4$. An example of such a basis is $\{x + 3, x\}$.

Example B.5. The ring $\mathbb{F}_2[x]/(x^4)$ has no σ-pseudo-self-dual bases, but has 12 symmetric bases over $\mathbb{F}_2$. An example of such a basis is $\{x^2+x, x^3+x, 1, x^3+1\}$.

Example B.6. The ring $\mathbb{F}_2[x]/(x^2 + y^2, xy)$ (see [14]) has 16 symmetric bases over $\mathbb{F}_2$. An example of such a basis is $\big(y^2 + 1, y, x, 1\big)$.

Example B.7. The ring $A = \mathbb{F}_2[x]/(x^2, y^2)$ has 8 symmetric basis over $\mathbb{F}_2$. An example of such a basis is $(y + 1, x + 1, xy + x + y + 1, 1)$. The ring A has also 7 subrings isomorphic to $\mathbb{F}_2[x]/(x^2)$. For the subring $R = \{0, 1, x, x + 1\}$ there are 48 symmetric bases of A over R. One such a basis is $(y + 1, x + 1)$ for which

$$M_{y+1} = \begin{pmatrix} 0 & x+1 \\ x+1 & 0 \end{pmatrix} \text{ and } M_{x+1} = \begin{pmatrix} x+1 & 0 \\ 0 & x+1 \end{pmatrix}.$$

Example B.8. The ring $\mathbb{F}_2[x]/(x^3)$ of order 8 has no self dual basis but has four symmetric bases: $\big(x^2+x, x^2+1, 1\big)$, $\big(x^2+1, x, 1\big)$, $\big(x^2+x, x+1, x^2+x+1\big)$, $\big(x, x+1, x^2+x+1\big)$

Example B.9. The ring $\mathbb{F}_2[x]/(x^3-1)$ of order 8 has no self dual basis but has three symmetric bases: $\big(x^2+1, x+1, x^2+x+1\big)$, $\big(x^2+x, x+1, x^2+x+1\big)$, $\big(x^2+x, x^2+1, x^2+x+1\big)$.

Example B.10. The self dual basis $(x, x+1)$ of the ring $\mathbb{F}_2[x]/(x^2+x)$ of order 4 is also a symmetric basis.

Example B.11. The ring $\mathbb{F}_2[x]/(x^2)$ of order 4 (cf. ([9])) has no σ-pseudo-self-dual basis but has the unique symmetric basis $(x+1, 1)$.

References

[1] Adel Alahmadi, Houda Sboui, Patrick Solé, and Olfa Yemen, *Cyclic codes over $M_2(\mathbb{F}_2)$*, J. Franklin Inst. **350** (2013), no. 9, 2837–2847. MR 3146951

[2] R. Alfaro and K. Dhul-Qarnayn, *Constructing self-dual codes over $\mathbb{F}_q[u]/(u^t)$*, Des. Codes Cryptogr. **74** (2015), no. 2, 453–465. MR 3302667

[3] Christine Bachoc, *Applications of coding theory to the construction of modular lattices*, J. Combin. Theory Ser. A **78** (1997), no. 1, 92–119. MR 1439633 (98a:11084)

[4] Katherine G. Bartley and Judy L. Walker, *Algebraic geometric codes over rings*, Advances in algebraic geometry codes, Ser. Coding Theory Cryptol., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 323–361. MR 2509128 (2010j:14051)

[5] Koichi Betsumiya, San Ling, and Fidel R. Nemenzo, *Type II codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$*, Discrete Math. **275** (2004), no. 1-3, 43–65. MR 2026275 (2004i:94051)

[6] A. Bonnecaze, E. Rains, and P. Solé, 3-*colored* 5-*designs and Z_4-codes*, J. Statist. Plann. Inference **86** (2000), no. 2, 349–368, Special issue in honor of Professor Ralph Stanton. MR 1768278 (2001g:05021)

[7] Delphine Boucher, Patrick Solé, and Felix Ulmer, *Skew constacyclic codes over Galois rings*, Adv. Math. Commun. **2** (2008), no. 3, 273–292. MR MR2429458

[8] A. R. Calderbank, A. Roger Hammons, Jr., P. Vijay Kumar, N. J. A. Sloane, and Patrick Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. Amer. Math. Soc. (N.S.) **29** (1993), no. 2, 218–222. MR MR1215307 (94b:94020)

[9] Steven T. Dougherty, Philippe Gaborit, Masaaki Harada, and Patrick Solé, *Type II codes over* $\mathbf{F}_2 + u\mathbf{F}_2$, IEEE Trans. Inform. Theory **45** (1999), no. 1, 32–45. MR 1677846 (2000h:94053)

[10] Philippe Gaborit and Ayoub Otmani, *Experimental constructions of self-dual codes*, Finite Fields Appl. **9** (2003), no. 3, 372–394. MR 1983055

[11] Jian Gao and Yun Gao, *Some results on linear codes over* $\mathbb{Z}_4 + \mathbb{Z}_4 v$, arXiv: http://arxiv.org/abs/1402.6771 (2014).

[12] Marcus Greferath, *Cyclic codes over finite rings*, Discrete Math. **177** (1997), no. 1-3, 273–277. MR 1483452

[13] San Ling and Patrick Solé, *Type II codes over* $\mathbf{F}_4 + u\mathbf{F}_4$, European J. Combin. **22** (2001), no. 7, 983–997. MR 1857260 (2002k:94040)

[14] Edgar Martínez-Moro and Steve Szabo, *On codes over local Frobenius non-chain rings of order 16*, Noncommutative Rings and Their Applications (Steven Dougherty, Alberto Facchni, André Leroy, Edmund Puczylowski, and Patrick Solé, eds.), Contemp. Math., vol. 634, Amer. Math. Soc., Providence, RI, 2015, pp. 227–243.

[15] Edgar Martínez-Moro, Steve Szabo, and Bahattin Yildiz, *Linear codes over* $\frac{\mathbb{Z}_4[x]}{\langle x^2+2x\rangle}$, Int. J. Inf. Coding Theory **3** (2015), no. 1, 78–96. MR 3341091

[16] C. Mouaha, *On q-ary images of self-dual codes*, Appl. Algebra Engrg. Comm. Comput. **3** (1992), no. 4, 311–319. MR 1325763 (96e:94019)

[17] Gadiel Seroussi and Abraham Lempel, *Factorization of symmetric matrices and trace-orthogonal bases in finite fields*, SIAM J. Comput. **9** (1980), no. 4, 758–767. MR 592766 (81k:15019)

[18] Steve Szabo and Jay Wood, *Properties of dual codes defined by nondegenerate forms*, to appear in Jacodesmath Journal (2016).

[19] Jay A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575. MR MR1738408 (2001d:94033)